PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-041280
(43)Date of publication of application : 12.02.1999

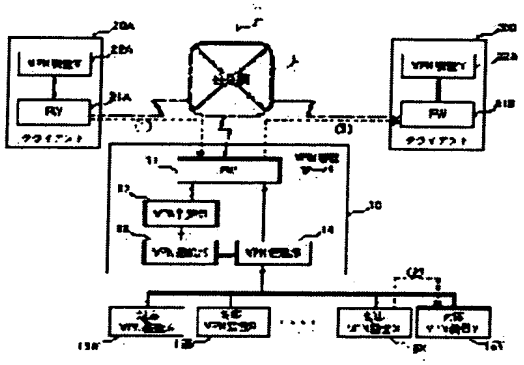
(51)Int.Cl. H04L 12/56
H04L 12/22
// G09C 1/00
H04L 9/36

(21)Application number : 09-190302
(22)Date of filing : 15.07.1997

(71)Applicant : N T T DATA:KK
(72)Inventor : MATSUDA YOSHIYUKI
KOBATA YASUHIRO
TSUBOI AKIHISA

(54) COMMUNICATION SYSTEM, VPN REPEATER AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication system in which different kinds of virtual private networks(VPN) are compatible.
SOLUTION: A communication system 1 is constituted by providing plural VPN devices 22A and 22B and a VPN managing server 10 equipped with correspondent VPN devices 15X, 15Y... for constructing the VPN on a communication network in cooperation with the respective VPN devices 22A and 22B. The VPN managing server 10 receives an enciphered telegraphic message by constructing the 1st VPN with the VPN device 22A of a telegraphic message transmission source and specifies the VPN device 22B of the transmission destination by deciphering the transmission destination information included in the received enciphered telegraphic message and at the same time, the 2nd VPN is constructed with the VPN device 22B of the transmission source. After the received enciphered telegraphic message is deciphered by a cryptographic key for the 1st VPN, this is enciphered by a cryptographic key for the 2nd VPN and transmitted through the 2nd VPN to the VPN device 22B.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－41280

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ａ
	12/22		Ｇ０９Ｃ	1/00	６６０Ｅ
// Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｌ	11/26	
Ｈ０４Ｌ	9/36			9/00	６８５

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平9－190302

(22)出願日　平成９年(1997)７月15日

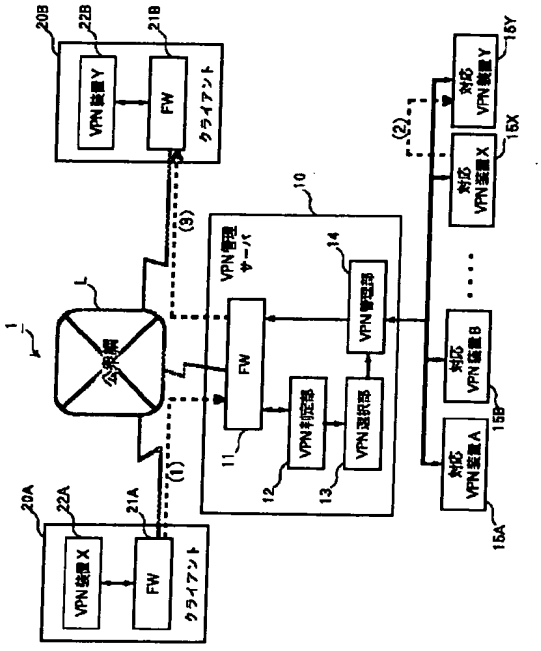
(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　松田　栄之
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　木幡　康弘
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　壷井　彰久
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　通信システム、ＶＰＮ中継装置、記録媒体

(57)【要約】

【課題】　異種のＶＰＮが互換可能な通信システムを提供する。

【解決手段】　複数のＶＰＮ装置２２Ａ，２２Ｂと、各ＶＰＮ装置２２Ａ，２２Ｂと協働して通信網上にＶＰＮを構築する対応ＶＰＮ装置１５Ｘ，１５Ｙ･･･を具備したＶＰＮ管理サーバ１０とを含んで通信システム１を構成する。ＶＰＮ管理サーバ１０は、電文送信元のＶＰＮ装置２２Ａとの間に第１ＶＰＮを構築して暗号電文を受信し、受信した暗号電文に含まれる送信先情報を解読して送信先のＶＰＮ装置２２Ｂを特定するとともに、該送信元のＶＰＮ装置２２Ｂとの間に第２ＶＰＮを構築する。そして、受信した暗号電文を第１ＶＰＮ用の暗号鍵で復号化した後、これを第２ＶＰＮ用の暗号鍵で暗号化し、第２ＶＰＮを通じてＶＰＮ装置２２Ｂに送信する。



【特許請求の範囲】

【請求項１】　それぞれ同一規格の対応ＶＰＮ装置との協働により通信網上にＶＰＮを構築する複数のＶＰＮ装置と、前記複数のＶＰＮ装置に対応するすべての対応ＶＰＮ装置を具備したＶＰＮ中継装置とを含み、

前記ＶＰＮ中継装置が、

電文送信元のＶＰＮ装置との間に第１ＶＰＮを構築して暗号電文を受信する手段と、受信した暗号電文に含まれる送信先情報を解読して送信先のＶＰＮ装置を特定するとともに、該送信元のＶＰＮ装置との間に第２ＶＰＮを構築する手段と、前記受信した暗号電文を第２ＶＰＮ用の暗号電文に変換して第２ＶＰＮに送出する手段とを備えて、各ＶＰＮ装置における電文送信の中継を行うように構成されていることを特徴とする通信システム。

【請求項２】　前記ＶＰＮ中継装置の前記暗号電文の入出力インタフェース部分にファイアウォールが介在することを特徴とする請求項１記載の通信システム。

【請求項３】　それぞれ同一規格のＶＰＮ装置との協働により通信網上にＶＰＮを構築する複数の対応ＶＰＮ装置と、

電文送信元となる第１ＶＰＮ装置との間に第１ＶＰＮ、電文送信先となる第２ＶＰＮ装置との間に第２ＶＰＮを、それぞれ該当する対応ＶＰＮ装置を用いて構築し、第１ＶＰＮを通じて受信した第１ＶＰＮ装置からの暗号電文を第２ＶＰＮ用の暗号電文に変換するとともに、変換した暗号電文を第２ＶＰＮを通じて第２ＶＰＮ装置へ送信する経路制御手段と、

を有することを特徴とするＶＰＮ中継装置。

【請求項４】　前記複数の対応ＶＰＮ装置は、それぞれ異なる認証手法、暗号鍵の交換手法、及び暗号化手法に基づいてＶＰＮ装置との間にＶＰＮを構築するものであり、前記経路制御手段は、予め用意されたこれらの対応ＶＰＮ装置から該当する装置を選択して前記第１ＶＰＮ及び第２ＶＰＮを構築することを特徴とする請求項３記載のＶＰＮ中継装置。

【請求項５】　前記経路制御手段は、前記第１ＶＰＮを通じて受信した暗号電文を前記第１ＶＰＮ装置の暗号鍵で復号化し、これにより得られた復号電文を前記第２ＶＰＮ装置の暗号鍵で暗号化して第２ＶＰＮへ送出することを特徴とする請求項３または４記載のＶＰＮ中継装置。

【請求項６】　それぞれ対応ＶＰＮ装置との協働により通信網上にＶＰＮを構築するＶＰＮ装置に相互通信可能に接続されたコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、

前記プログラムが、

電文送信元となる第１ＶＰＮ装置との間に第１ＶＰＮを構築して暗号電文を受信する処理、

受信した暗号電文に含まれる送信先情報を解読して送信先の通信装置を特定するとともに、該送信先となる第２ＶＰＮ装置との間に第２ＶＰＮを構築する処理、及び、前記受信した暗号電文を第２ＶＰＮ用の暗号電文に変換して第２ＶＰＮに送出する処理を前記コンピュータ装置に実行させるものであることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信網上にＶＰＮ（Virtual Private Network：仮想専用回線）を構築してデータ通信を行う通信システムに関し、特に、ＶＰＮを構築するＶＰＮ装置の規格差を吸収する技術に関する。

【０００２】

【従来の技術】例えば広域ネットワーク環境を利用した通信システムでは、不正侵入者に対する機密保護等を考慮した高信頼のシステム構築及び運用管理が望まれている。ここに広域ネットワーク環境とは、インターネット等のような広域通信網（ネットワーク）上で送信先経路を制御するルータを介して通信装置相互間のデータ通信を行う環境をいう。ルータは、伝送対象電文の先頭に付加された送信先と送信元のアドレスに基づいて送信先への経路の最適な選択を行う装置である。このようなルータをベースにしたネットワークとしては、企業等の組織内ネットワークや、インターネット・プロバイダのような不特定多数の者に対してネットワーク接続環境を提供するものもあり、その形態は多様化している。また、電話やファクシミリ等に代わる低コストの新たな通信手段として電子メールも定着してきている。このように、今後、電話等の従来回線をネットワーク環境で代替したシステム構築の要求は、急激に増加する傾向にある。

【０００３】しかし、広域ネットワーク環境下でのデータ通信では、第三者によるデータ傍受やデータ改竄が容易に起こりうるため、セキュリティ面で問題がある。そのため、例えばエレクトリックコマースの分野で使用される電子通貨のように、機密性の高いデータを通信媒体を用いて伝送しあう場合は、別途、専用回線を敷設する必要があった。そこで、最近は、データ暗号技術、認証技術、対象データを隠蔽するカプセル化技術等を応用し、広域ネットワーク上にＶＰＮを構築してデータ通信を行う技術が提案されている。

【０００４】図５は、広域ネットワークである公衆網Ｌ上にＶＰＮを構築してデータ通信を行う従来の通信システムの一例を示す概念図である。この通信システム２は、データの送受信機能を備えたコンピュータ装置４０，５０、ＶＰＮ装置４１，５１、ファイアウォール（ＦＷ）４２，５２、及びルータ４３，５３を具備して構成される。ＦＷ４２，５２は、外部からの不正なアクセスに対する保護を特殊なソフトウェアで実現した一種の障壁であり、公衆網Ｌのような広域ネットワークを使用する環境においては必須なものとなっている。

【０００５】通信システム４において、コンピュータ装

置４０から遠隔地にある他のコンピュータ装置５０に対して電文送信を行う場合の手順は以下のようになる。まず、送信元及び送信先のルータ４３，５３間で相互に認証処理を行い、さらに、送信元及び送信先のＶＰＮ装置４１，５１間で、暗号鍵の相互交換を行う。そして、送信元のＶＰＮ装置４１において、送信先のＶＰＮ装置４１の暗号鍵を用いて電文を暗号化して送信する。一方、送信先のＶＰＮ装置５１では、暗号化された電文を受信するとともに、当該電文を送信元のＶＰＮ装置５１の暗号鍵で復号化してコンピュータ装置５０に転送する。

【０００６】なお、ＶＰＮ装置４１，５１には、他のＶＰＮ装置を相互に確認する認証機能、暗号化のための暗号鍵交換機能、電文の暗号化・復号化機能のほか、ルータとしての機能を具備したものもある。これらの機能は、メーカによる独自方式、或いは標準化方式によって実現されている。また、ＶＰＮ装置によっては、暗号鍵交換機能を有しないものもあり、必ずしも統一された規格に準拠していないのが現状である。

【０００７】

【発明が解決しようとする課題】ところで、ＶＰＮ装置４１，５１に具備される認証機能、暗号鍵交換機能、暗号化・復号化等の各機能における規格等の標準化は進められてはいるが、上述のように、現在は、メーカ毎の独自の規格で各機能が実現されて製品化されているため、異なるメーカの製品間ではＶＰＮを構築することができない。そのため、例えば既にＶＰＮ装置を導入している複数の異業種企業が合同のＶＰＮによるネットワーク環境（以下、ＶＰＮ環境）を構築しようとする場合、同一メーカの製品を使用すれば問題なくＶＰＮ環境が構築可能であるが、異なるメーカの製品間では、そのままではＶＰＮ環境の構築は不可能である。

【０００８】そこで本発明の課題は、異種のＶＰＮ装置を使用してもＶＰＮ環境を構築できる、改良された通信システムを提供することにある。本発明の他の課題は、異種のＶＰＮ装置を使用した通信システムにおいて、ＶＰＮ環境を容易に構築できるＶＰＮ中継装置、及びこのＶＰＮ中継装置を汎用のコンピュータ装置で実現するための記録媒体を提供することにある。

【０００９】

【課題を解決するための手段】上記課題を解決する本発明の通信システムは、それぞれ同一規格の対応ＶＰＮ装置との協働により通信網上にＶＰＮを構築する複数のＶＰＮ装置と、前記複数のＶＰＮ装置に対応するすべての対応ＶＰＮ装置を具備したＶＰＮ中継装置とを含み、前記ＶＰＮ中継装置が、電文送信元のＶＰＮ装置との間に第１ＶＰＮを構築して暗号電文を受信する手段と、受信した暗号電文に含まれる送信先情報を解読して送信先のＶＰＮ装置を特定するとともに、該送信元のＶＰＮ装置との間に第２ＶＰＮを構築する手段と、前記受信した暗号電文を第２ＶＰＮ用の暗号電文に変換して第２ＶＰＮに送出する手段とを備えて、各ＶＰＮ装置間の電文送信の中継を行うように構成されることを特徴とする。

【００１０】なお、前記ＶＰＮ中継装置の前記暗号電文の入出力インタフェース部分には、ファイアウォールが介在するようにする。

【００１１】上記他の課題を解決する本発明のＶＰＮ中継装置は、それぞれ同一規格のＶＰＮ装置との協働により通信網上にＶＰＮを構築する複数の対応ＶＰＮ装置と、電文送信元となる第１ＶＰＮ装置との間に第１ＶＰＮ、電文送信先となる第２ＶＰＮ装置との間に第２ＶＰＮを、それぞれ該当する対応ＶＰＮ装置を用いて構築し、第１ＶＰＮを通じて受信した第１ＶＰＮ装置からの暗号電文を第２ＶＰＮ用の暗号電文に変換するとともに、変換した暗号電文を第２ＶＰＮを通じて第２ＶＰＮ装置へ送信する経路制御手段と、を有することを特徴とする。暗号電文の変換は、例えば前記第１ＶＰＮを通じて受信した暗号電文を前記第１ＶＰＮ装置の暗号鍵で復号化し、これにより得られた復号電文を前記第２ＶＰＮ装置の暗号鍵で暗号化することにより行う。

【００１２】なお、前記複数の対応ＶＰＮ装置は、それぞれ異なる認証手法、暗号鍵の交換手法、及び暗号化手法に基づいてＶＰＮ装置との間にＶＰＮを構築するものであり、前記経路制御手段は、予め用意されたこれらの対応ＶＰＮ装置から該当する装置を選択して前記第１ＶＰＮ及び第２ＶＰＮを構築する。

【００１３】上記他の課題を解決する本発明の記録媒体は、それぞれ対応ＶＰＮ装置との協働により通信網上にＶＰＮを構築するＶＰＮ装置に相互通信可能に接続されたコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、前記プログラムが、下記の処理を当該コンピュータ装置に実行させるものである。

（１）電文送信元となる第１ＶＰＮ装置との間に第１ＶＰＮを構築して暗号電文を受信する処理、（２）受信した暗号電文に含まれる送信先情報を解読して送信先の通信装置を特定するとともに、該送信先となる第２ＶＰＮ装置との間に第２ＶＰＮを構築する処理、（３）前記受信した暗号電文を第２ＶＰＮ用の暗号電文に変換して第２ＶＰＮに送出する処理。

【００１４】

【発明の実施の形態】以下、本発明を広域ネットワークによる通信システムに適用した場合の実施の形態を、図面を参照して詳細に説明する。図１は、本実施形態の通信システムの機能ブロック図である。この通信システム１は、電文の送受信を行う複数のクライアント２０Ａ，２０Ｂと、本発明のＶＰＮ中継装置であるＶＰＮ管理サーバ１０とを公衆網Ｌを介して双方向通信可能に接続されて構成される。各クライアント２０Ａ，２０Ｂは、ＦＷ２１Ａ，２１Ｂ及びＶＰＮ装置２２Ａ，２２Ｂを具備する通信装置である。

【００１５】ＶＰＮ管理サーバ１０は、それぞれ異なる

メーカにより独自の規格で製品化された複数の対応ＶＰＮ装置１５Ａ，１５Ｂ，・・・１５Ｘ，１５Ｙ（以下、特定の対応ＶＰＮ装置を指す場合以外は、サフィックスを除去した符号１５を用いる）が接続された汎用のコンピュータ装置と、このコンピュータ装置に読み取られて実行されたときに、前述のＦＷ１１、ＶＰＮ判定部１２、ＶＰＮ選択部１３、及びＶＰＮ管理部１４の機能を実現するコンピュータプログラムとからなる。このコンピュータプログラムは、通常、コンピュータ装置の内部記憶装置あるいは外部記憶装置に格納され、随時読み取られて実行されるようになっているが、コンピュータ装置とは分離可能な記録媒体、例えばＣＤ－ＲＯＭやＦＤ等に格納され、使用時に上記内部記憶装置または外部記憶装置にインストールされて随時実行に供されるものであってもよい。

【００１６】なお、本実施形態において、ＶＰＮ管理サーバ１０及び各クライアント２０は、各々、既存のルータに相当する通信制御手段を具備しているものとする。また、本実施形態において、各対応ＶＰＮ装置１５は、製品パッケージとして独立に存在し、それぞれ独自の規格によってＶＰＮ構築機能を発揮する場合と、ＶＰＮ管理サーバ１０の内部あるいは外部記憶装置に複数且つ異種のＶＰＮソフトウェア（プログラム）を格納しておき、該当するＶＰＮソフトウエアが随時読み出されて実行されることによってＶＰＮ構築機能を発揮する場合のいずれであってもよい。

【００１７】ＶＰＮ判定部１２は、送信元または送信先の各ＶＰＮ装置２２Ａ，２２Ｂに対応するサーバ側の対応ＶＰＮ装置１５が具備されているかどうかを判定するものである。ＶＰＮ選択部１３は、ＶＰＮ管理サーバ１０が具備している複数の対応ＶＰＮ装置１５から、送信元または送信先のＶＰＮ装置２２Ａ，２２Ｂに対応するものを選択するものである。ＶＰＮ管理部１４は、個々の対応ＶＰＮ装置１５の統括制御、認証処理、その他のデータ管理を行うものである。

【００１８】次に、本実施形態の通信システム１において、クライアント２０Ａ，２０Ｂ間で暗号電文の送受を行う場合の処理手順を図２を参照して説明する。この例では、クライアント２０ＡではＶＰＮ装置Ｘ（２２Ａ）を使用し、クライアント２０Ｂ側では、ＶＰＮ装置Ｘと規格が異なるＶＰＮ装置Ｙ（２２Ｂ）を使用するものとする。また、送信対象となる電文に付与されるアドレス情報には、送信先及び送信元のＶＰＮ装置Ｘ，Ｙ（１５Ｘ，２２Ａ，２２Ｂ，１５Ｙ）によるアドレス情報が使用され、電文に付与される元来のアドレス情報及びデータは、ＶＰＮ上では暗号化の対象となる。

【００１９】いま、クライアント２０Ａから図３（ａ）に示すフォーマットの電文がＶＰＮ管理サーバ１０に向けて送信されたとする（図１の（１））。ＶＰＮ管理サーバ１０は、ＦＷ１１を介して受信した電文をＶＰＮ判定部１２に送る（ステップＳ１０１）。ＶＰＮ判定部１２は、この電文に付与されたアドレス情報から、クライアント２０ＡのＶＰＮ装置２２Ａと協働してＶＰＮを構築するための対応ＶＰＮ装置がサーバ内に具備されているか否か、つまり、ＶＰＮ装置Ｘと対になる対応ＶＰＮ装置Ｘが存在するか否かを判定する（ステップＳ１０２）。

【００２０】対になる対応ＶＰＮ装置ＸがＶＰＮ管理サーバ１０に具備されている場合は、ＶＰＮ選択部１２で、複数のＶＰＮ１５から該当するものを選択する。この場合の選択方法としては、具体的には、ＶＰＮ管理サーバ１０に具備されている複数のＶＰＮ装置１５に関する情報を予めＶＰＮ選択部１２に保持しておき、当該情報と電文に付与されるアドレス情報とを比較し、合致するものを選択するようにする。本例では、ＶＰＮ装置Ｘ（２２Ａ）と対になる対応ＶＰＮ装置Ｘ（１５Ｘ）が存在しているので、これを選択する。この選択情報は、ＶＰＮ管理部１４に入力される。

【００２１】ＶＰＮ管理部１４は、選択した対応ＶＰＮ装置１５Ｘを起動させ、ＶＰＮ装置２２Ａとの間にＶＰＮを構築する（ステップＳ１０２：Yes、Ｓ１０３）。そして、受信した電文の暗号化部分を、ＶＰＮ装置１５Ｘの暗号鍵（ＶＰＮ装置２２Ａとの間で交換した暗号鍵）で復号化し（ステップＳ１０４）、図３（ｂ）のようなフォーマットの復号電文を得る。この復号電文から元来の送信先のクライアント２０Ｂを特定するとともに、ＶＰＮ判定部１２でそのクライアントのＶＰＮ装置Ｙ（２２Ｂ）と対になる対応ＶＰＮ装置ＹがＶＰＮ管理サーバ１０に具備されているか否かを判定する（ステップＳ１０５）。対になる対応ＶＰＮ装置ＹがＶＰＮ管理サーバ１０に具備されている場合は、ＶＰＮ選択部１２で、該当するものを選択し、ＶＰＮ管理部１４がその対応ＶＰＮ装置Ｙ（１５Ｙ）を起動する（ステップＳ１０５：Yes、Ｓ１０６）。そして、対応ＶＰＮ装置１５Ｙに復号電文を渡して（図１の（２））これを対応ＶＰＮ装置の暗号鍵（ＶＰＮ装置２２Ｂとの間で交換した暗号鍵）で暗号化し、さらにこの暗号電文に送信先及び送信元のアドレス情報を付与してＦＷ１１を介してクライアント２０Ｂに送信する（ステップＳ１０７）。このときの電文フォーマットは図３（ｃ）に示すとおりである。これにより、クライアント２０Ｂは、クライアント２０Ａからの電文を取得することができる。なお、ステップＳ１０２及びステップＳ１０５において、対応ＶＰＮ装置Ｘ，ＹがＶＰＮ管理サーバ１０に具備されていない場合は、送信元のクライアント２０Ａにエラー通知を行う（ステップＳ１０８）。以上の処理をすべての電文について繰り返す（ステップＳ１０９）。

【００２２】図４は、本実施形態の通信システム１の概念図である。通常、ＶＰＮは、通信を行うクライアント間に直接構築されるが、本実施形態では、図４に示され

るように、複数地点Ａ～Ｄに存在するクライアントとＶＰＮ管理サーバ１０との間にそれぞれＶＰＮを構築し、クライアント間の通信は、常にＶＰＮ管理サーバ１０を経由してこのＶＰＮを通じて行うようにしている。ＶＰＮ管理サーバ１０は、各地点のクライアント側のＶＰＮ装置に対応する複数の対応ＶＰＮ装置を具備しており、各クライアント側のＶＰＮ装置間の規格差は、このＶＰＮ管理サーバ１０で吸収されるので、送信元のクライアントは、送信先のクライアント側のＶＰＮ装置の規格を意識することなく、電文を送信することが可能になる。

【００２３】このように、本実施形態の通信システム１では、ＶＰＮ管理サーバ１０が、受信した暗号電文を送信元のＶＰＮ装置２２Ａと対になる対応ＶＰＮ装置１５Ｘで復号化するとともに、復号電文を送信先のＶＰＮ装置２２Ｂと対になる対応ＶＰＮ装置１５Ｙで暗号化してＶＰＮ装置２２Ｂに送信するので、異種のＶＰＮ装置間の認証機能、暗号鍵交換機能、暗号化・復号化機能等の互換が可能となる。また、対応ＶＰＮ装置によって異なる暗号鍵を用いた復号化及び暗号化を行うので、機密保護能力の低下も防止することができる。従って、複数地点間において異なるメーカのＶＰＮ装置により構築された異種ＶＰＮの使用が可能になり、従来の問題点が解消される。

【００２４】なお、本実施形態では、便宜上、クライアント２０Ａからクライアント２０Ｂへ、異なるＶＰＮ装置Ｘ，Ｙ（２２Ａ，２２Ｂ）を使用して暗号電文を送信する通信システムの例を説明したが、クライアント２０Ｂからクライアント２０Ａに暗号電文を送信する場合、あるいは、各クライアント２０Ａ，２０ＢのＶＰＮ装置が同一規格の場合も同様の手順で電文送信が可能になる。

【００２５】

【発明の効果】以上の説明から明らかなように、本発明によれば、ＶＰＮ管理サーバにおいて、送信元及び送信先のＶＰＮ装置との間にＶＰＮが構築する対応ＶＰＮ装置が選択されて電文送信の中継が行われるので、異種のＶＰＮ装置を使用した場合であってもＶＰＮ環境の構築が可能となる効果がある。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る通信システムの機能ブロック図。

【図２】ＶＰＮ管理サーバにおける電文中継の手順説明図。

【図３】（ａ）は送信元のクライアントからＶＰＮ管理サーバに送信される電文のフォーマット、（ｂ）はＶＰＮ管理サーバ内で復号された電文のフォーマット、（ｃ）はＶＰＮ管理サーバから元来の送信先となるクライアントに送信される電文のフォーマットを示す図。

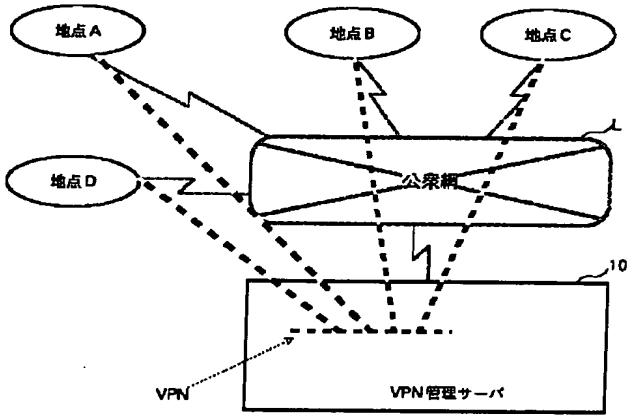
【図４】本実施形態の通信システムにおける動作の概念説明図。

【図５】ＶＰＮを使用した従来型の通信システムにおける機能ブロック図。

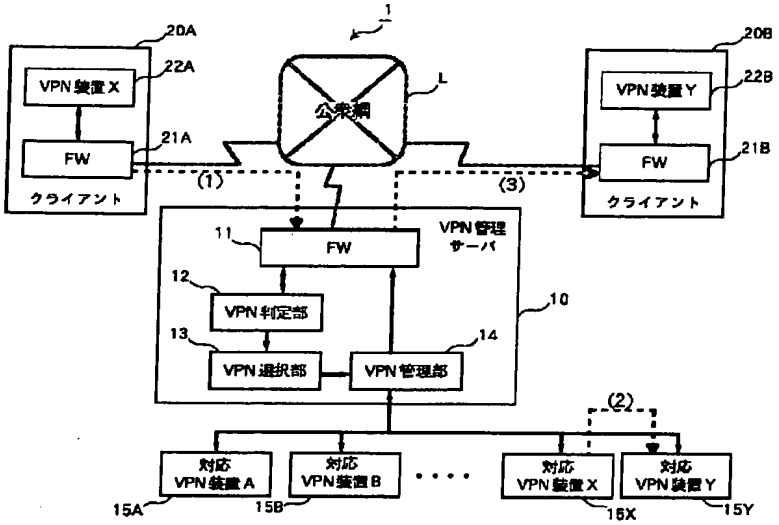
【符号の説明】

１　通信システム
１０　ＶＰＮ管理サーバ
１１，２１Ａ，２１Ｂ　ファイアウォール（ＦＷ）
１２　ＶＰＮ判定部
１３　ＶＰＮ選択部
１４　ＶＰＮ管理部
１５Ａ，１５Ｂ，…１５Ｘ，１５Ｙ　対応ＶＰＮ装置
２０Ａ，２０Ｂ　クライアント
２２Ａ，２２Ｂ　ＶＰＮ装置

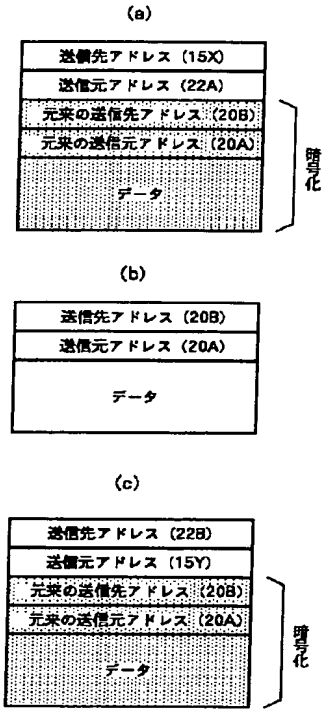
【図４】



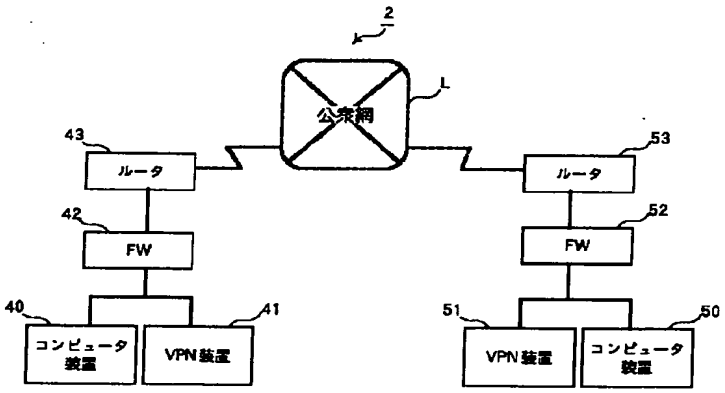
【図１】


1
20A
VPN装置X
22A
FW
21A
クライアント
公衆網
L
20B
VPN装置Y
22B
FW
21B
クライアント
(1)
(3)
VPN管理サーバ
11
FW
12
VPN判定部
13
VPN選択部
14
VPN管理部
10
(2)
対応VPN装置A
15A
対応VPN装置B
15B
対応VPN装置X
15X
対応VPN装置Y
15Y

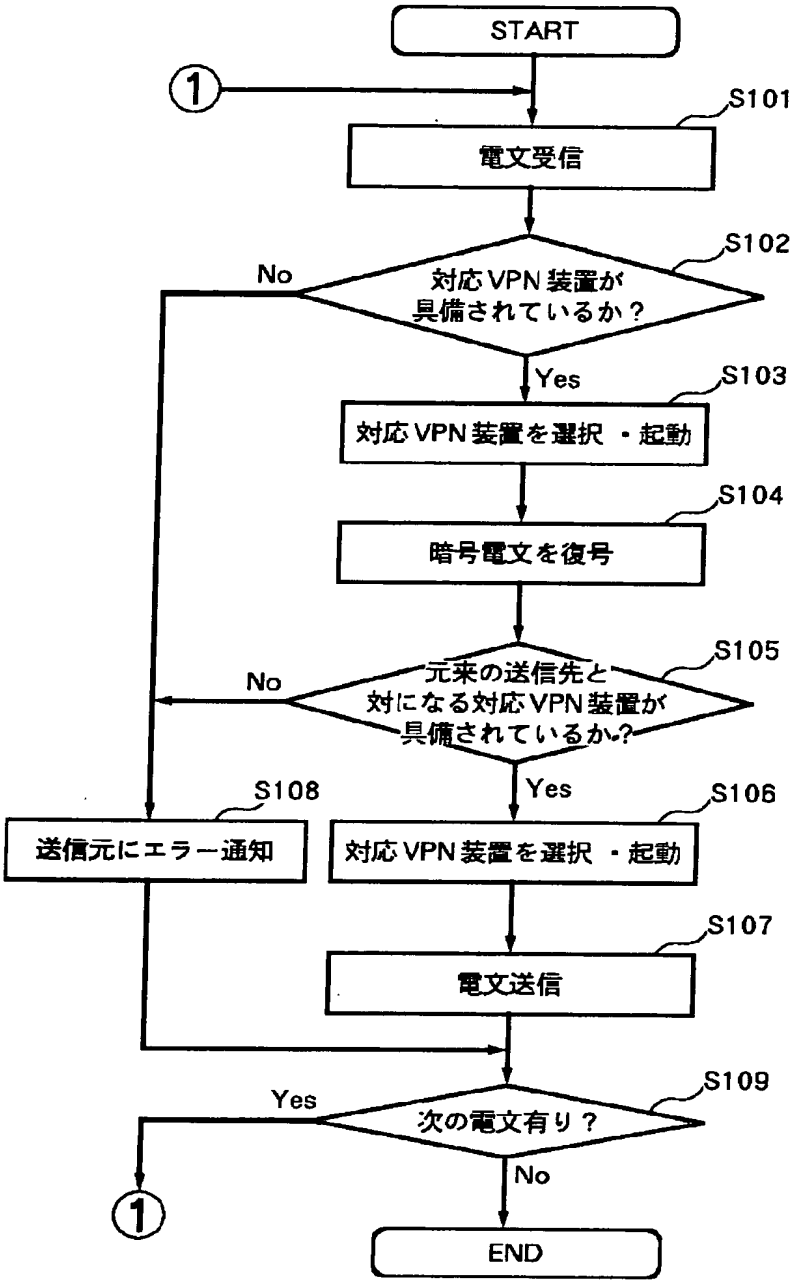
【図３】


(a)
送信先アドレス（15X）
送信元アドレス（22A）
元来の送信先アドレス（20B）
元来の送信元アドレス（20A）
データ
暗号化
(b)
送信先アドレス（20B）
送信元アドレス（20A）
データ
(c)
送信先アドレス（22B）
送信元アドレス（15Y）
元来の送信先アドレス（20B）
元来の送信元アドレス（20A）
データ
暗号化

【図５】


2
公衆網
L
43
ルータ
42
FW
40
コンピュータ装置
41
VPN装置
53
ルータ
52
FW
51
VPN装置
50
コンピュータ装置

【図２】


START
①
S101
電文受信
S102
No
対応VPN装置が
具備されているか？
Yes
S103
対応VPN装置を選択・起動
S104
暗号電文を復号
S105
No
元来の送信先と
対になる対応VPN装置が
具備されているか？
Yes
S108
送信元にエラー通知
S106
対応VPN装置を選択・起動
S107
電文送信
S109
Yes
次の電文有り？
No
①
END